

APPLICATION
FOR
UNITED STATES LETTERS PATENT

TITLE: ENABLING OPTIONAL SYSTEM FEATURES
APPLICANT: TODD A. SCHELLING AND MAHESH S. NATU

CERTIFICATE OF MAILING BY EXPRESS MAIL

Express Mail Label No. ET371085988US

I hereby certify that this correspondence is being deposited with the United States Postal Service as Express Mail Post Office to Addressee with sufficient postage on the date indicated below and is addressed to the Commissioner for Patents, Washington, D.C. 20231.

Date of Deposit

May 10, 2001

Signature

Gil Vargas

Typed or Printed Name of Person Signing Certificate

ENABLING OPTIONAL SYSTEM FEATURES

TECHNICAL FIELD

This invention relates to enabling optional system
5 features.

BACKGROUND

The BIOS (Basic Input/Output System) of a computer is a collection of low-level, machine dependent software that serves to isolate an operating system (e.g., MS-DOS on a personal computer) from the details of the hardware. For example, the BIOS includes procedural calls that read from and write to an absolute disk address, read a character from the keyboard, and write a character to the screen. The BIOS is typically placed on a non-volatile memory chip, e.g., ROM (Read-Only Memory), flash memory, and EEPROM (Electrically Erasable Programmable ROM), supplied by a computer manufacture. The contents of the non-volatile chip are not affected when the computer is powered off. The BIOS is usually stored separately from the OS (Operating System) of the computer to allow independent upgrade
20 of the OS and the BIOS.

Because BIOS of newer versions can be developed during the life span of a computer, it may be necessary to upgrade the BIOS

for enhanced performance. Therefore, most modern personal computers store the BIOS on a re-writable memory chip. In particular, a flash memory chip is most often adopted because of its simplicity in use and efficiency to update.

5 Some computer manufacturers add a RAM (Random Access Memory) for use by the BIOS because RAMs are in general faster than most of the non-volatile memory chips. Each time the computer is rebooted, the BIOS is copied from the non-volatile memory chip to the RAM to accelerate operations of the BIOS. The copying procedure is also known as a "shadowing" procedure.

10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995
1000
1005
1010
1015
1020
1025
1030
1035
1040
1045
1050
1055
1060
1065
1070
1075
1080
1085
1090
1095
1100
1105
1110
1115
1120
1125
1130
1135
1140
1145
1150
1155
1160
1165
1170
1175
1180
1185
1190
1195
1200
1205
1210
1215
1220
1225
1230
1235
1240
1245
1250
1255
1260
1265
1270
1275
1280
1285
1290
1295
1300
1305
1310
1315
1320
1325
1330
1335
1340
1345
1350
1355
1360
1365
1370
1375
1380
1385
1390
1395
1400
1405
1410
1415
1420
1425
1430
1435
1440
1445
1450
1455
1460
1465
1470
1475
1480
1485
1490
1495
1500
1505
1510
1515
1520
1525
1530
1535
1540
1545
1550
1555
1560
1565
1570
1575
1580
1585
1590
1595
1600
1605
1610
1615
1620
1625
1630
1635
1640
1645
1650
1655
1660
1665
1670
1675
1680
1685
1690
1695
1700
1705
1710
1715
1720
1725
1730
1735
1740
1745
1750
1755
1760
1765
1770
1775
1780
1785
1790
1795
1800
1805
1810
1815
1820
1825
1830
1835
1840
1845
1850
1855
1860
1865
1870
1875
1880
1885
1890
1895
1900
1905
1910
1915
1920
1925
1930
1935
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
2030
2035
2040
2045
2050
2055
2060
2065
2070
2075
2080
2085
2090
2095
2100
2105
2110
2115
2120
2125
2130
2135
2140
2145
2150
2155
2160
2165
2170
2175
2180
2185
2190
2195
2200
2205
2210
2215
2220
2225
2230
2235
2240
2245
2250
2255
2260
2265
2270
2275
2280
2285
2290
2295
2300
2305
2310
2315
2320
2325
2330
2335
2340
2345
2350
2355
2360
2365
2370
2375
2380
2385
2390
2395
2400
2405
2410
2415
2420
2425
2430
2435
2440
2445
2450
2455
2460
2465
2470
2475
2480
2485
2490
2495
2500
2505
2510
2515
2520
2525
2530
2535
2540
2545
2550
2555
2560
2565
2570
2575
2580
2585
2590
2595
2600
2605
2610
2615
2620
2625
2630
2635
2640
2645
2650
2655
2660
2665
2670
2675
2680
2685
2690
2695
2700
2705
2710
2715
2720
2725
2730
2735
2740
2745
2750
2755
2760
2765
2770
2775
2780
2785
2790
2795
2800
2805
2810
2815
2820
2825
2830
2835
2840
2845
2850
2855
2860
2865
2870
2875
2880
2885
2890
2895
2900
2905
2910
2915
2920
2925
2930
2935
2940
2945
2950
2955
2960
2965
2970
2975
2980
2985
2990
2995
3000
3005
3010
3015
3020
3025
3030
3035
3040
3045
3050
3055
3060
3065
3070
3075
3080
3085
3090
3095
3100
3105
3110
3115
3120
3125
3130
3135
3140
3145
3150
3155
3160
3165
3170
3175
3180
3185
3190
3195
3200
3205
3210
3215
3220
3225
3230
3235
3240
3245
3250
3255
3260
3265
3270
3275
3280
3285
3290
3295
3300
3305
3310
3315
3320
3325
3330
3335
3340
3345
3350
3355
3360
3365
3370
3375
3380
3385
3390
3395
3400
3405
3410
3415
3420
3425
3430
3435
3440
3445
3450
3455
3460
3465
3470
3475
3480
3485
3490
3495
3500
3505
3510
3515
3520
3525
3530
3535
3540
3545
3550
3555
3560
3565
3570
3575
3580
3585
3590
3595
3600
3605
3610
3615
3620
3625
3630
3635
3640
3645
3650
3655
3660
3665
3670
3675
3680
3685
3690
3695
3700
3705
3710
3715
3720
3725
3730
3735
3740
3745
3750
3755
3760
3765
3770
3775
3780
3785
3790
3795
3800
3805
3810
3815
3820
3825
3830
3835
3840
3845
3850
3855
3860
3865
3870
3875
3880
3885
3890
3895
3900
3905
3910
3915
3920
3925
3930
3935
3940
3945
3950
3955
3960
3965
3970
3975
3980
3985
3990
3995
4000
4005
4010
4015
4020
4025
4030
4035
4040
4045
4050
4055
4060
4065
4070
4075
4080
4085
4090
4095
4100
4105
4110
4115
4120
4125
4130
4135
4140
4145
4150
4155
4160
4165
4170
4175
4180
4185
4190
4195
4200
4205
4210
4215
4220
4225
4230
4235
4240
4245
4250
4255
4260
4265
4270
4275
4280
4285
4290
4295
4300
4305
4310
4315
4320
4325
4330
4335
4340
4345
4350
4355
4360
4365
4370
4375
4380
4385
4390
4395
4400
4405
4410
4415
4420
4425
4430
4435
4440
4445
4450
4455
4460
4465
4470
4475
4480
4485
4490
4495
4500
4505
4510
4515
4520
4525
4530
4535
4540
4545
4550
4555
4560
4565
4570
4575
4580
4585
4590
4595
4600
4605
4610
4615
4620
4625
4630
4635
4640
4645
4650
4655
4660
4665
4670
4675
4680
4685
4690
4695
4700
4705
4710
4715
4720
4725
4730
4735
4740
4745
4750
4755
4760
4765
4770
4775
4780
4785
4790
4795
4800
4805
4810
4815
4820
4825
4830
4835
4840
4845
4850
4855
4860
4865
4870
4875
4880
4885
4890
4895
4900
4905
4910
4915
4920
4925
4930
4935
4940
4945
4950
4955
4960
4965
4970
4975
4980
4985
4990
4995
5000
5005
5010
5015
5020
5025
5030
5035
5040
5045
5050
5055
5060
5065
5070
5075
5080
5085
5090
5095
5100
5105
5110
5115
5120
5125
5130
5135
5140
5145
5150
5155
5160
5165
5170
5175
5180
5185
5190
5195
5200
5205
5210
5215
5220
5225
5230
5235
5240
5245
5250
5255
5260
5265
5270
5275
5280
5285
5290
5295
5300
5305
5310
5315
5320
5325
5330
5335
5340
5345
5350
5355
5360
5365
5370
5375
5380
5385
5390
5395
5400
5405
5410
5415
5420
5425
5430
5435
5440
5445
5450
5455
5460
5465
5470
5475
5480
5485
5490
5495
5500
5505
5510
5515
5520
5525
5530
5535
5540
5545
5550
5555
5560
5565
5570
5575
5580
5585
5590
5595
5600
5605
5610
5615
5620
5625
5630
5635
5640
5645
5650
5655
5660
5665
5670
5675
5680
5685
5690
5695
5700
5705
5710
5715
5720
5725
5730
5735
5740
5745
5750
5755
5760
5765
5770
5775
5780
5785
5790
5795
5800
5805
5810
5815
5820
5825
5830
5835
5840
5845
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
5920
5925
5930
5935
5940
5945
5950
5955
5960
5965
5970
5975
5980
5985
5990
5995
6000
6005
6010
6015
6020
6025
6030
6035
6040
6045
6050
6055
6060
6065
6070
6075
6080
6085
6090
6095
6100
6105
6110
6115
6120
6125
6130
6135
6140
6145
6150
6155
6160
6165
6170
6175
6180
6185
6190
6195
6200
6205
6210
6215
6220
6225
6230
6235
6240
6245
6250
6255
6260
6265
6270
6275
6280
6285
6290
6295
6300
6305
6310
6315
6320
6325
6330
6335
6340
6345
6350
6355
6360
6365
6370
6375
6380
6385
6390
6395
6400
6405
6410
6415
6420
6425
6430
6435
6440
6445
6450
6455
6460
6465
6470
6475
6480
6485
6490
6495
6500
6505
6510
6515
6520
6525
6530
6535
6540
6545
6550
6555
6560
6565
6570
6575
6580
6585
6590
6595
6600
6605
6610
6615
6620
6625
6630
6635
6640
6645
6650
6655
6660
6665
6670
6675
6680
6685
6690
6695
6700
6705
6710
6715
6720
6725
6730
6735
6740
6745
6750
6755
6760
6765
6770
6775
6780
6785
6790
6795
6800
6805
6810
6815
6820
6825
6830
6835
6840
6845
6850
6855
6860
6865
6870
6875
6880
6885
6890
6895
6900
6905
6910
6915
6920
6925
6930
6935
6940
6945
6950
6955
6960
6965
6970
6975
6980
6985
6990
6995
7000
7005
7010
7015
7020
7025
7030
7035
7040
7045
7050
7055
7060
7065
7070
7075
7080
7085
7090
7095
7100
7105
7110
7115
7120
7125
7130
7135
7140
7145
7150
7155
7160
7165
7170
7175
7180
7185
7190
7195
7200
7205
7210
7215
7220
7225
7230
7235
7240
7245
7250
7255
7260
7265
7270
7275
7280
7285
7290
7295
7300
7305
7310
7315
7320
7325
7330
7335
7340
7345
7350
7355
7360
7365
7370
7375
7380
7385
7390
7395
7400
7405
7410
7415
7420
7425
7430
7435
7440
7445
7450
7455
7460
7465
7470
7475
7480
7485
7490
7495
7500
7505
7510
7515
7520
7525
7530
7535
7540
7545
7550
7555
7560
7565
7570
7575
7580
7585
7590
7595
7600
7605
7610
7615
7620
7625
7630
7635
7640
7645
7650
7655
7660
7665
7670
7675
7680
7685
7690
7695
7700
7705
7710
7715
7720
7725
7730
7735
7740
7745
7750
7755
7760
7765
7770
7775
7780
7785
7790
7795
7800
7805
7810
7815
7820
7825
7830
7835
7840
7845
7850
7855
7860
7865
7870
7875
7880
7885
7890
7895
7900
7905
7910
7915
7920
7925
7930
7935
7940
7945
7950
7955
7960
7965
7970
7975
7980
7985
7990
7995
8000
8005
8010
8015
8020
8025
8030
8035
8040
8045
8050
8055
8060
8065
8070
8075
8080
8085
8090
8095
8100
8105
8110
8115
8120
8125
8130
8135
8140
8145
8150
8155
8160
8165
8170
8175
8180
8185
8190
8195
8200
8205
8210
8215
8220
8225
8230
8235
8240
8245
8250
8255
8260
8265
8270
8275
8280
8285
8290
8295
8300
8305
8310
8315
8320
8325
8330
8335
8340
8345
8350
8355
8360
8365
8370
8375
8380
8385
8390
8395
8400
8405
8410
8415
8420
8425
8430
8435
8440
8445
8450
8455
8460
8465
8470
8475
8480
8485
8490
8495
8500
8505
8510
8515
8520
8525
8530
8535
8540
8545
8550
8555
8560
8565
8570
8575
8580
8585
8590
8595
8600
8605
8610
8615
8620
8625
8630
8635
8640
8645
8650
8655
8660
8665
8670
8675
8680
8685
8690
8695
8700
8705
8710
8715
8720
8725
8730
8735
8740
8745
8750
8755
8760
8765
8770
8775
8780
8785
8790
8795
8800
8805
8810
8815
8820
8825
8830
8835
8840
8845
8850
8855
8860
8865
8870
8875
8880
8885
8890
8895
8900
8905
8910
8915
8920
8925
8930
8935
8940
8945
8950
8955
8960
8965
8970
8975
8980
8985
8990
8995
9000
9005
9010
9015
9020
9025
9030
9035
9040
9045
9050
9055
9060
9065
9070
9075
9080
9085
9090
9095
9100
9105
9110
9115
9120
9125
9130
9135
9140
9145
9150
9155
9160
9165
9170
9175
9180
9185
9190
9195
9200
9205
9210
9215
9220
9225
9230
9235
9240
9245
9250
9255
9260
9265
9270
9275
9280
9285
9290
9295
9300
9305
9310
9315
9320
9325
9330
9335
9340
9345
9350
9355
9360
9365
9370
9375
9380
9385
9390
9395
9400
9405
9410
9415
9420
9425
9430
9435
9440
9445
9450
9455
9460
9465
9470
9475
9480
9485
9490
9495
9500
9505
9510
9515
9520
9525
9530
9535
9540
9545
9550
9555
9560
9565
9570
9575
9580
9585
9590
9595
9600
9605
9610
9615
9620
9625
9630
9635
9640
9645
9650
9655
9660
9665
9670
9675
9680
9685
9690
9695
9700
9705
9710
9715
9720
9725
9730
9735
9740
9745
9750
9755
9760
9765
9770
9775
9780
9785
9790
9795
9800
9805
9810
9815
9820
9825
9830
9835
9840
9845
9850
9855
9860
9865
9870
9875
9880
9885
9890
9895
9900
9905
9910
9915
9920
9925
9930
9935
9940
9945
9950
9955
9960
9965
9970
9975
9980
9985
9990
9995
10000
10005
10010
10015
10020
10025
10030
10035
10040
10045
10050
10055
10060
10065
10070
10075
10080
10085
10090
10095
10100
10105
10110
10115
10120
10125
10130
10135
10140
10145
10150
10155
10160
10165
10170
10175
10180
10185
10190
10195
10200
10205
10210
10215
10220
10225
10230
10235
102

FIG. 2 shows a process for enabling the optional system features.

DETAILED DESCRIPTION

Referring to FIG. 1, a processing system 10 includes a BIOS memory 12, an OS (Operating System) memory 13, and system resources 25. OS memory 13 stores an OS 33, which manages system resources 25 and contains high-level software to provide a user-friendly programming environment. BIOS memory 12 stores a BIOS 22, which is a collection of device drivers that allow users of system 10 and OS 33 to interact with the hardware of the system, but hide machine-dependent details from them. An exemplary memory for BIOS memory 12 is a flash memory, which is re-writable. System resources 25 includes elements of system 10 that contribute to processing power, storage capacity, redundancy, and speed, e.g., memory, input/output devices, processors, redundant power supplies, and PCI (Peripheral Component Interconnect) bus.

Some of system resources 25 have system features that can be optionally selected or configured on an as-needed basis. The features generally include on/off status of the elements of system 10 and adjustable parameters of these elements, e.g., memory size, number of processors, number of PCI slots, PCI bus speed, number of redundant power supplies, and processor speed.

In certain scenarios, it is desirable to selectively enable some of the system features as needed for run-time usage. For example, a manufacturer, e.g., an OEM (Original Equipment Manufacturer), can produce computer systems with the same number of processors. When an end-user purchases one of the computer systems but only uses a few of the processors for performing tasks, the OEM can enable the number of processors as needed by the user. In general, the OEM can produce computer systems with uniform resources and configurations, and can enable the system features selectively after client needs and cost options are determined. The capability of enabling optional system features can be useful in situations where an end-user wants to rent or lease system capacity, performance, or manageability as an alternative to outright purchasing these features. This capability can also be useful when a system provider wishes to reduce the number of available stocked computers, each having different system features, for a given hardware/software set. The number of different stocked computers can be reduced by differentiating the identical computers by enabling different system features. Furthermore, this capability also allows end-users to update or upgrade system capacity or system features without opening the system.

The capability of enabling optional system features is preferably secure, because the OEM may not want the system

features to be enabled without authorization. For security purposes, system 10 includes a write-once non-volatile storage 31. Storage 31 is protected from write and erase operations. For example, storage 31 can be a flash memory protected by chipset options, e.g., SMI (System Management Interrupt) protection. The SMI is a special and high-priority interrupt in a PC AT bus architecture that prevents any non-BIOS software application from writing or erasing storage 31.

Storage 31 stores a decryption key 310, a public key 311, and GUID 312 (Globally Unique Identifier). GUID 312 is a long identifier, e.g., 128 bytes, which uniquely identifies system 10. BIOS 22 uses the above contents of storage 31 to implement a secure environment; specifically, the secure environment guarantees authenticity, privacy, and validation of messages from the OEM. The secure environment assures that a message from the OEM for enabling system features will be received and processed in a secure manner.

A BIOS-based control mechanism, as will be described in detail below, is used to provide the capability of enabling optional system features in a secure manner. BIOS 22 includes a flash update code 23 that accesses the contents of storage 31. BIOS 22 also includes a feature set 24 where status of the system features are recorded. In one embodiment, BIOS update code 23 includes a decryption function 232 that decrypts the

message sent from the OEM, an authentication function 233 that authenticates a digital signature of the message, a verification function 234 that verifies the message, and a flash update utility 235 that updates a secure non-volatile storage 32.

5 Operations of flash update code 23 will be discussed in detail below.

When the OEM of system 10 wishes to enable certain features of the system, the OEM sends a message to BIOS 22. The message can be transmitted to BIOS 22 in a number of ways, for example, through a network in the form of "feature packets" 27, on a floppy diskette inserted into a floppy drive of system 10, using a file copy, or by electronic mail. Regardless how the message is transmitted to BIOS 22, it is important that the authenticity, validity, and privacy when appropriate, of the message be guaranteed. The authenticity, validity, and privacy of the feature packet's content are protected by encryption and digital signature. Because of the protection of the encryption and digital signature, it is not required that the message be transmitted via secure mechanisms. The BIOS 22 at the final destination of the feature packet (i.e., system 10) can perform complete authentication and validation of the feature packet's content regardless of the transmission medium and/or number of time the feature packet is transferred. Furthermore, the

privacy of the feature packet's content is guaranteed at all times as a result of the encryption.

Specifically, when the OEM sends the message to BIOS 22, the OEM generates a digital signature with a private key known only to the OEM. The digital signature is attached to the message to assure the recipient (i.e., BIOS 22) that the message is from an authentic sender. When BIOS 22 receives the message, authentication function 233 uses a public key 311 to confirm that the digital signature is correct, valid, and has not been tampered with. If the content of the message also requires privacy, the OEM can encrypt the message with an encryption key using an encryption algorithm (e.g., 128-bit RSA) to guarantee privacy of the message. When BIOS 22 receives the message, decryption function 232 uses decryption key 310, which is known only to system 10, to decrypt the received message. The encryption ensures that the message will not be meaningful to anyone other than the intended recipient.

In addition to authenticity and privacy, the recipient also needs to verify that it is indeed the intended recipient of the message. Therefore, the message from the sender also includes an identifier that will be verified against GUID 312. Only the message with an identifier matching the GUID of system 10 will be processed by BIOS 22.

Referring to FIG. 2, an example of a process 40 is shown for enabling optional system features of system resources 25. BIOS 22 receives a message from the OEM, for example, in the form of feature packets 27 arriving from a network connected to system 10 (block 41). If the message is encrypted, decryption function 232 decrypts the message using decryption key 310 (block 42). Authentication function 233 authenticates the digital signature in the message using public key 311 (block 43). Verification function 234 verifies the identifier in the message against GUID 312 (block 44). If failure occurs (blocks 411, 412, and 413) during the decryption, authentication, or verification, process 40 is aborted, and the message is discarded (block 49).

If no failure occurs, in one scenario, BIOS 22 executes flash update utility 235 to write the message into a secure non-volatile storage 32 (block 45), which only accepts inputs from a trusted source, e.g., BIOS 22. System 10 is then rebooted (block 46). During the rebooting process, BIOS 22 retrieves the information in storage 32 and executes according to the information to enable optional system features (block 47). BIOS 22 then records the optional system features in feature set 24 (block 48).

It should be noted that while reboot at block 46 is shown in process 40, in certain scenarios, system 10 does not need to

be rebooted. With appropriate stack support from OS 33 and software, system 10 can continue to operate while the system features are being enabled. However, one benefit of rebooting the system is that the current OS 33 and hardware can be used in this BIOS-based control mechanism without modifications.

At block 45 of process 40, secure non-volatile storage 32 can be connected to system 10 either locally, or remotely via network links. Storage 32 serves as a database that stores the decrypted and validated message from the OEM. Only a trusted source, e.g., BIOS 22, can write or erase the contents of storage 32. In one embodiment, storage 32 identifies BIOS 22 as the trusted source, and accepts any input coming from BIOS 22. In another embodiment, BIOS 22 encrypts the message before it is sent to storage 32, and storage 32 decrypts the message in the same manner as performed by decryption function 232. Other techniques for ensuring the trust between BIOS 22 and storage 32 are also possible. Examples of storage 32 include a flash memory, an EEPROM, and a disk, or any other device that is secure, non-volatile, and re-writable.

In certain scenarios, BIOS 22 does not need to write the message to storage 32, and therefore can skip block 45 of process 40. For example, if the message from the OEM contains BIOS-executable code, BIOS 22 can splice the code into its normal execution path, thus effectively modifying itself or

erasing part of itself in response to the message. This "splicing" approach is better suited for controlling system features such as number of processors or memory sizes. In another approach, the message from the OEM can include executable code that can be used as DLL (Dynamically Loaded Library). The code is stored in a flash portion of system 10, and is loaded by BIOS 22 at run-time. The "DLL" approach allows BIOS 22 to patch itself with the new executable code, and is better suited for adding large new functionalities such as adding hot-plug CPU (Central Processing Unit) support, or hot-plug memory support.

In embodiments where processing system 10 includes multiple processors, feature set 24 includes an MPS (Multiple Processor Specification) table 241 for storing features related to the multiple processors, e.g., number of processors, processing speed of each of the processors, and so forth. For example, assume that the message from the OEM specifies that only a few of the processors in system 10 will be authorized and enabled. In one scenario, BIOS 22 disables the un-authorized processors by a sequence of actions in an implementation-specific manner. The sequence of actions may include asserting the FLUSH# during a reset, asserting the STP_CLK#, omitting the processors from the MPS and/or ACPI (Advanced Configuration and Power management Interface) processor tables. Once system 10 has been fully

rebooted, all the authorized processors will be enabled. The status of the enabled/disabled processors is then recorded in MPS table 241 of feature set 24.

5 In certain scenarios, if any of the specified processors fail in the above multiple-processor embodiments, BIOS 22 can detect these failed processors and enable spare processors to ensure the correct number of processors being enabled whenever possible.

10 Other optional system features that can be controlled by the BIOS-based control mechanism include, e.g., amount of system memory, number of powered PCI slots, speed of processors, speed of specific PCI buses, as well as enabling serviceability features, embedded PCI devices such as SCSI (Small Computer System Interface), video, LAN (Local Area Network), peripheral ports such as parallel, USB (Universal Serial Bus) keyboard, mouse, hot-plug PCI, and hot-plug CPU or memory nodes. Even OS
15 level application features can be enabled by the BIOS-based control mechanism in a substantially the same manner. Although some of these features can be enabled directly from system 10
20 without the feature packets from the OEM, some of the features are so complicated that direct enabling may be infeasible. These complicated features are generally implementation-specific so that a third party agent, e.g., a computer distributor, cannot practically enable the system features without detailed

knowledge of the hardware. Therefore, the BIOS-based control mechanism for enabling optional system features, as described above, also has an advantage for simplifying configuration procedures for the parties that do not possess comprehensive knowledge of the hardware.

Other embodiments are within the scope of the following claims.